**In the Claims:**

Following is a complete listing of the claims pending in the application, as amended:

1. – 139. (Cancelled)

140. (Previously Presented) A method performed by a server of a public key system, said public key system further comprising a plurality of client terminals, said method comprising the steps of:

storing a first list of fingerprints of digitally encoded data;

computing a first fingerprint for at least a part of said list of fingerprints; and

providing said computed first fingerprint.

141. (Previously Presented) The method according to claim 140, wherein said step of computing said first fingerprint comprises the steps of:

obtaining one or more entries of said first list of fingerprints, whereby said one or more entries are to be covered by said first fingerprint; and

computing a hash value on at least said obtained one or more entries.

142. (Previously Presented) The method according to claim 140, wherein said first list of fingerprints further comprises at least one of the following:

a unique identifier associated with each fingerprint;

a time specification associated with each fingerprint, whereby said time specification specifies at least one of a time of entry into said first list associated with said fingerprint or said digital data, a time of generation of said fingerprint or said digital data, or a time of provision of said fingerprint or said digital data to said server; or

a link to digital data or an association with digital data of each fingerprint.

143. (Previously Presented) The method according to claim 141, wherein said one or more entries in said step of obtaining said computed first fingerprint further comprising at least one of a unique identifier or a time specification associated with a fingerprint.

144. (Previously Presented) The method according to claim 142, wherein said unique identifier, said time specification, said link or said association are established and assigned by said server as part of said storing step.

145. (Previously Presented) The method according to claim 140, wherein said step of providing said computed first fingerprint comprises attaching said first fingerprint to a message that is sent to at least one of said plurality of user terminals.

146. (Previously Presented) The method according to claim 140, wherein said step of providing said computed first fingerprint or said step of computing said first fingerprint further comprises signing said first fingerprint by said server.

147. (Previously Presented) The method according to claim 140, wherein said step of storing a first list of fingerprints comprises the steps of:

receiving digital data;

establishing at least one of the integrity of said digital data, the identity of a sender of said digital data and the authenticity of said sender; whereby said establishing comprises at least one of verifying a digital signature for said digital data, verifying a fingerprint associated with said digital data or sender, using a secure and trusted connection for the communication with said sender, and applying an encryption scheme for the said received digital data;

computing a hash value on at least said digital data; and

adding said hash value to said first list of fingerprints.

148. (Previously Presented) The method according to claim 140, wherein at least said steps of computing a first fingerprint and providing said computed first fingerprint are performed repeatedly according to a timed schedule, and wherein said first list of fingerprints can be augmented or continued with further entries.

149. (Previously Presented) The method according to claim 148, wherein said step of providing said computed first fingerprint comprises providing or updating said first fingerprint on an hourly, daily, weekly, monthly or another regular time period basis.

150. (Previously Presented) The method according to claim 140, wherein said step of providing said computed first fingerprint further comprises associating and providing at least one of a time specification, a validity period information or another identifier providing for establishing the validity of said provisioned first fingerprint.

151. (Previously Presented) A method performed by a client terminal of a public key system, said public key system comprising a plurality of client terminals and at least one server, said method comprising the steps of:

obtaining a first list of fingerprints of digitally encoded data from a first source;

obtaining a first fingerprint of said list of fingerprints from a first source;

obtaining a second fingerprint of said list of fingerprints from a second source; and

comparing said first and said second fingerprint.

152. (Previously Presented) The method according to claim 151, further comprising the steps of:

computing a fingerprint of said obtained first list of fingerprints;

comparing said computed fingerprint and said obtained first and second fingerprints;

if at least one of said comparing steps result in different fingerprints, establishing that the data integrity of said received fingerprints or said first list of fingerprints has been compromised;

153. (Previously Presented) The method according to claim 151, further comprising the steps of:

obtaining at least one of said digitally encoded data of said fingerprint list;

computing a fingerprint of said obtained digital data;

comparing said computed fingerprint with the fingerprint for said obtained digital data in said received list of fingerprints; and

if said comparing step results in different fingerprints, establishing that the data integrity of said received digital data or said list of fingerprints has been compromised;

154. (Previously Presented) The method according to claim 151, further comprising at least one of:

verifying a digital signature for said received first and second fingerprint;

verifying a digital signature for a received list of fingerprints;

verifying a fingerprint associated with said received first and second fingerprint or said first and second source; and

receiving a user input to perform at least one of said steps of verifying a digital signature and verifying a fingerprint.

155. (Previously Presented) The method according to claim 151, wherein said steps of obtaining said first and second fingerprint comprising a step of

receiving said first and second fingerprint together with a message sent to said client terminal via communications media of a public network connecting said client terminals and said server; and

said method further comprising a step of:

attaching a fingerprint of said list of fingerprints to a message sent to another client terminal via said communications media of a public network connecting said client terminals.

156. (Previously Presented) The method according to claim 155, wherein said steps of obtaining said first and second fingerprint and attaching a fingerprint are accomplished automatically without an explicit request by the receiving client terminal of said message but as part of a regular communication between client terminals not established for the purpose of exchanging said first or second fingerprint.

157. (Previously Presented) The method according to claim 151, wherein said step of attaching a fingerprint further comprises associating and attaching at least one of a time specification, a validity period information or another identifier providing for establishing the validity of said provisioned fingerprint.

158. (Previously Presented) The method according to claim 155, wherein said step of attaching a fingerprint to a message is only performed for fingerprints that are verified by said client terminal to be valid and authentic; whereby said verification may depend on the number of successful comparing steps that were performed for said attached fingerprint with received corresponding fingerprints of mutually different and/or independent sources; and wherein said step of attaching a fingerprint further comprises signing said fingerprint by said client terminal using a private key of said client terminal.

159. (Previously Presented) The method according to claim 151, wherein said steps of obtaining said first and second fingerprint comprising a step of

determining whether a received fingerprint and/or a received list of fingerprints is valid and represents the latest published version by means of associated or attached information to said received fingerprint and/or received list of fingerprints or by means of a predetermined timed schedule known to said client terminal; and

if said received fingerprint and/or a received list of fingerprints is not valid, disregarding said received fingerprint and/or received list of fingerprints or

requesting a fingerprint and/or a list of fingerprints from another source to replace the invalid versions.

160. – 273. (Canceled)